(12) UK Patent Application (19) GB (11) 2 330 991 (13) A

(43) Date of A Publication 05.05.1999

(21) Application No 9723154.2

(22) Date of Filing 04.11.1997

(51) INT CL[6]
H04L 12/56 12/66

(52) UK CL (Edition Q)
H4P PPA PPEB

(56) Documents Cited
GB 2309561 A GB 2306862 A EP 0570630 A1
EP 0511926 A1 US 5623601 A US 5559883 A

(58) Field of Search
UK CL (Edition P) H4P PPA PPEB
INT CL[6] H04L 12/46 12/56 12/66 29/06
Online : WPI

(71) Applicant(s)
International Business Machines Corporation
(Incorporated in USA - New York)
Armonk, New York 10504, United States of America

(72) Inventor(s)
Andrew James Victor Yeomans

(74) Agent and/or Address for Service
J D Williams
IBM United Kingdom Limited, Intellectual Property
Department, Mail Point 110, Hursley Park,
WINCHESTER, Hampshire, SO21 2JN,
United Kingdom

(54) Abstract Title
Routing data packets

(57) Apparatus for re-routing a data packet 270 received from a source 140 on a first network 40 having a proxy server 80 and addressed to a destination 225 on a second network, e.g. via the internet 10, forwards the data packet to the proxy server 80 instead of the destination addressed in response to the data packet satisfying predetermined criteria, e.g. a source address on the first network, or a destination address on the second network, or a protocol type of the data packet. The criteria are stored in a routing table in the router 20, which provides a firewall function.

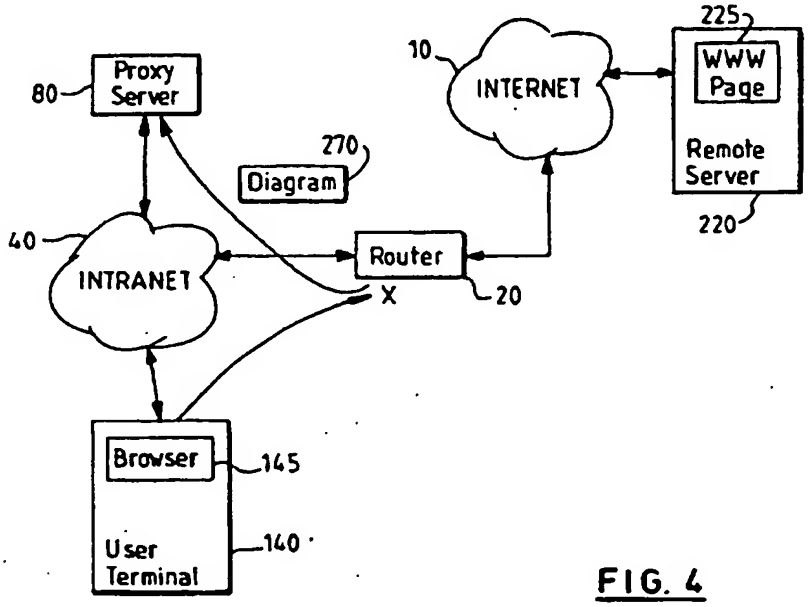

FIG. 4

GB 2 330 991 A

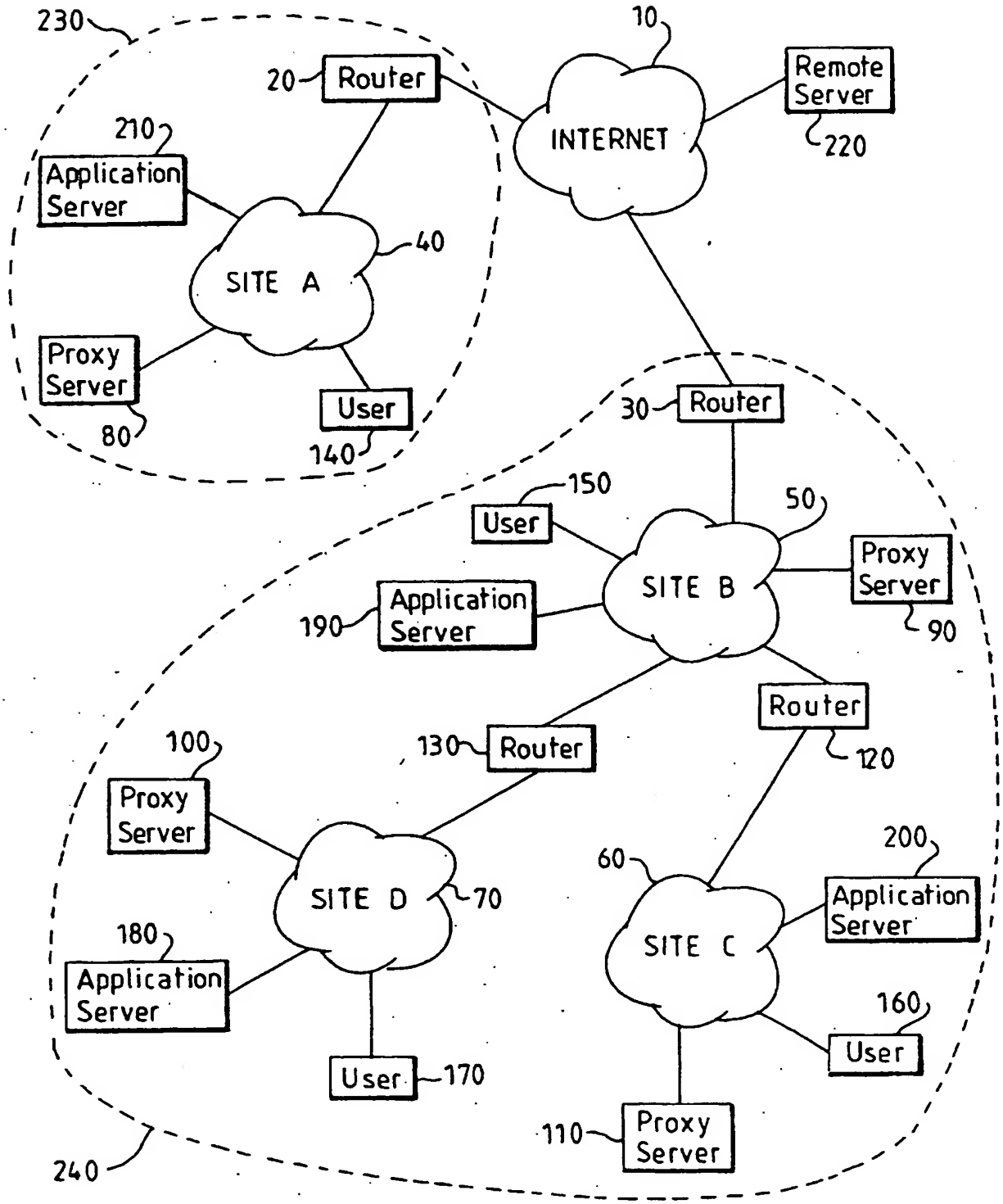

FIG. 1

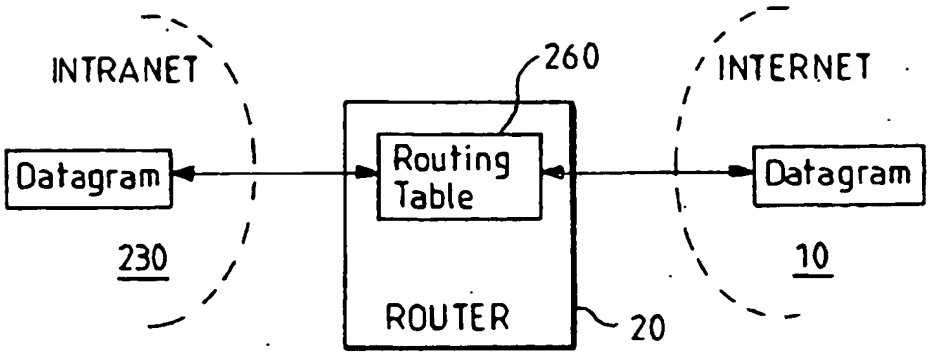

FIG. 2

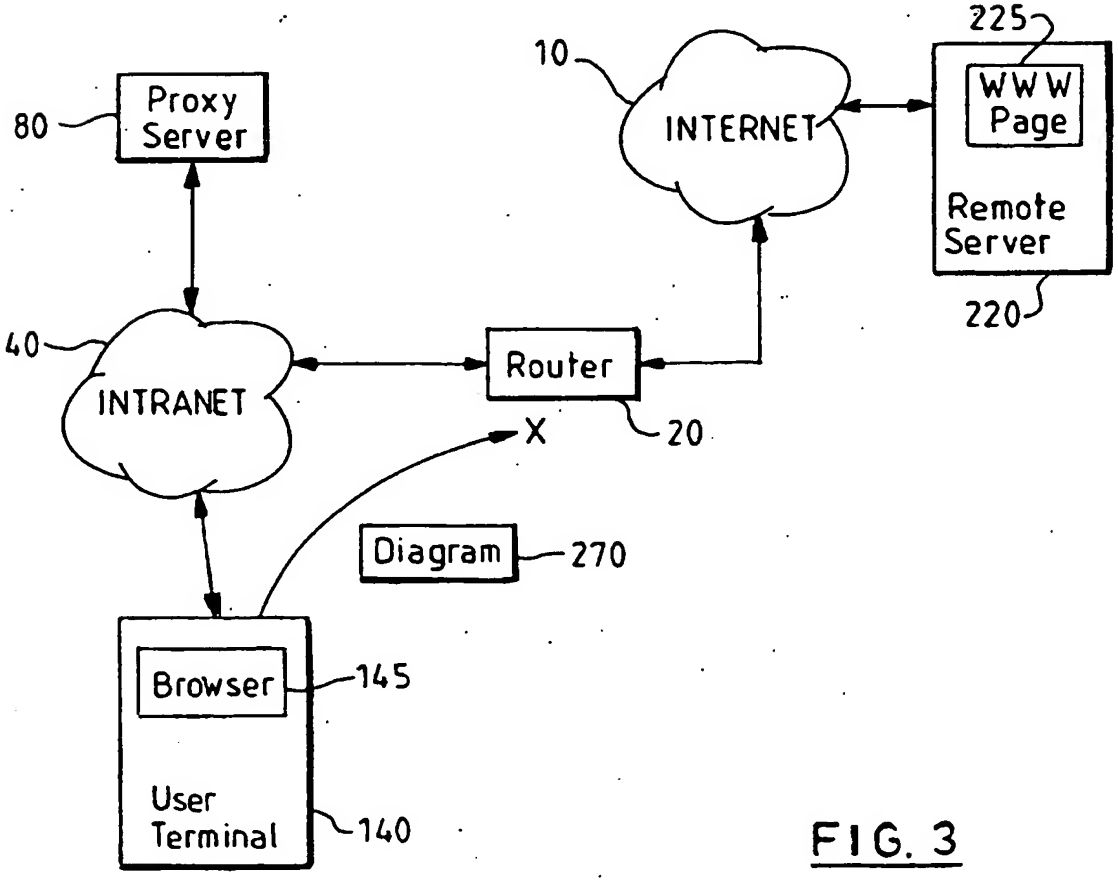

FIG. 3

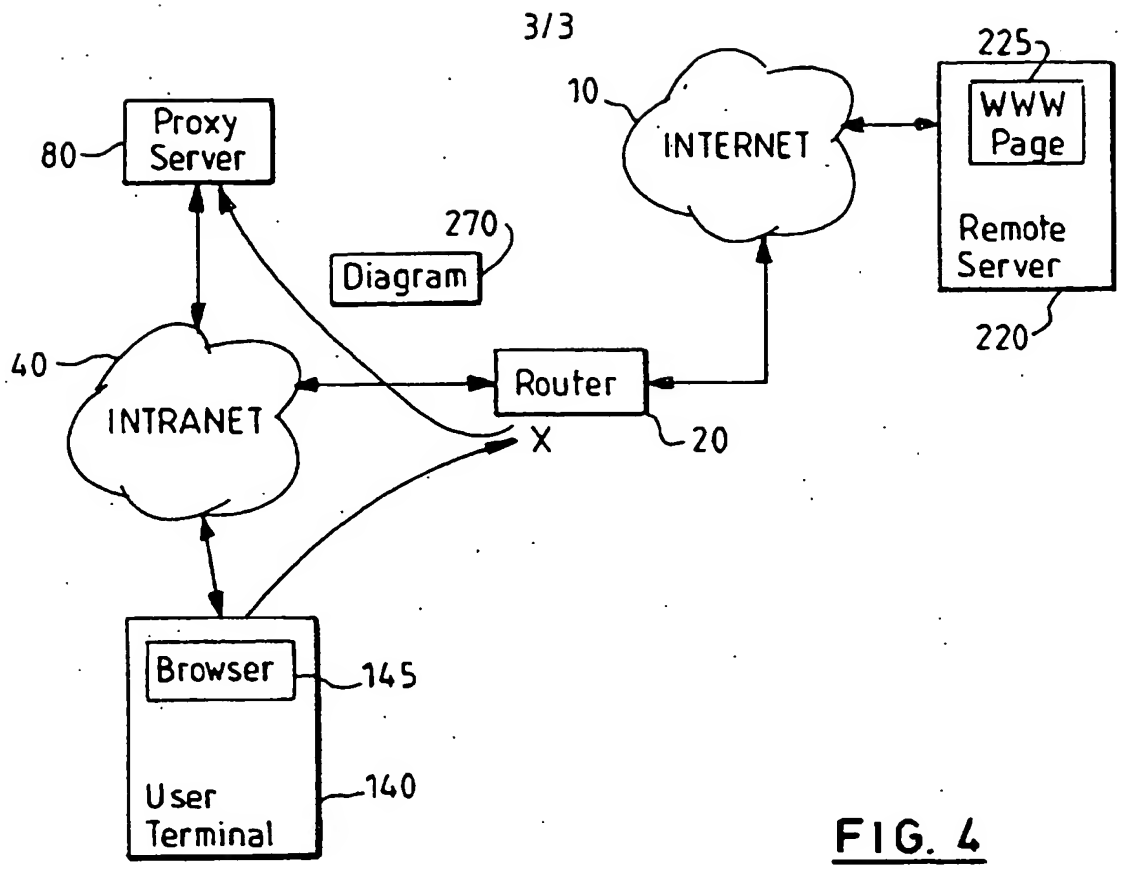

FIG. 4

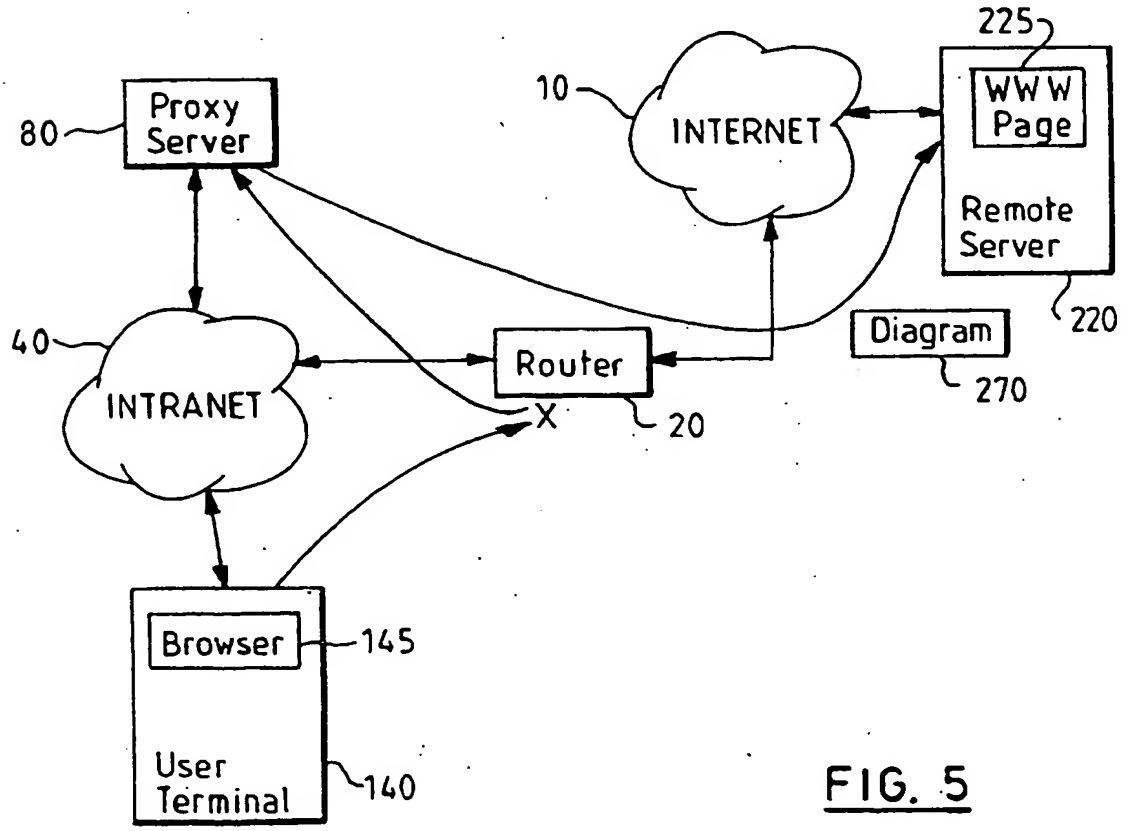

FIG. 5

2330991

METHOD AND APPARATUS FOR ROUTING DATA PACKETS

The present invention relates to a method and apparatus for routing data packets in a computer network.

A typical commercial computer network comprises a plurality of user terminals and server computers interconnected by local area network (LAN). Examples of typical LAN topologies are Ethernet and Token Ring. Increasingly, commercial organisation are recognising business advantages in Internet connectivity. Therefore the LAN is typically also coupled to the Internet.

The Internet is a global, public access data communications network comprising approximately 50,000 member networks in 100 countries. There are an estimated 30 million users of the Internet with thousands more being connected every day.

In general, data is communicated between end-points over the Internet in a packet form defined by the Transmission Control Protocol/Internet Protocol (TCP/IP). Each end-point connected to the Internet is identified by a unique Internet Protocol (IP) address. Each IP data packet is known as a datagram. Each datagram comprises a header portion and a data portion. The header portion contains the IP address of the source of the datagram and the IP address of the destination of the datagram.

The coupling between the LAN and the Internet is typically completed by a router. A router is interworking element for routing datagrams between networks according to source and destination IP addresses specified in the datagrams. In larger organisations, a plurality of LANs may be interconnected via routers to form an "intranet". One or more of the LANs in the intranet are typically connected to the Internet via additional routers. Typically, a proxy server computer system is connected to each LAN of the intranet. Each proxy server provided networking services to user terminals connected to the corresponding LAN. A router element may be integrated with a proxy server to form an application gateway.

It is desirable, in the interests of security, for the topology of an intranet to be arranged so that all data communications between computers on the intranet and computers on the intranet are made via the

proxy server. Thus, direct communications between computers on the Internet and computers on the intranet are prevented. Any suspicious data communication can be identified by the proxy server and appropriate action taken. The proxy server interprets protocol traffic and makes connections in the recipient network on behalf of the requesting computer. There is an application level connection between the requesting computer and the proxy server and, in turn, between the proxy server and the recipient computer. Conventionally, this arrangement can be implemented by configuring all networking software on the intranet to send all communications via the proxy server. However, in practice, such configuration is difficult to achieve because: intranet topologies change as updated hardware is introduced; users may configure their terminals incorrectly; and, users move from one location to another.

In accordance with the present invention there is now provided apparatus for routing a data packet received from a source on a first network having a proxy server and addressed to a destination on a second network, the apparatus comprising means for forwarding the data packet to the proxy server instead of the destination addressed in response to the data packet satisfying predetermined criteria.

Because, in accordance with the present invention, a data packet is forwarded to the proxy server instead of the destination addressed in response to the data packet satisfying predetermined criteria, a user terminal need not be reconfigured each time the network topology is changed. The present invention permits convenient maintenance of security options and network management at the proxy server in a manner which is transparent to users connecting to the network.

The forwarding means preferably comprises a routing table for storing the predetermined criteria. The predetermined criteria may comprise a source address on the first network. Equally, the predetermined criteria may comprise a destination address on the second network. Likewise, the predetermined criteria may comprise a protocol type of the data packet.

It will be appreciated that the present invention extends to a router comprising apparatus as hereinbefore described.

Viewing the present invention form another aspect, there is now provided a method for routing a data packet, the method comprising:

receiving the data packet from a source on a first network having a proxy server and addressed to a destination on a second network; and, forwarding the data packet to the proxy server instead of the destination addressed in response to the data packet satisfying predetermined criteria. Such a method preferably comprises storing the predetermined criteria in a routing table.

Preferred embodiments of the present invention will now be described by way of example only with reference to the accompanying drawings in which:

Figure 1 is a block diagram of a computer network;

Figure 2 is a simplified block diagram of a router;

Figure 3 is a block diagram of a subsection of the computer network shown in Figure 1;

Figure 4 is another block diagram of the network subsection shown in Figure 2; and,

Figure 5 is yet another block diagram of the network subsection shown in Figure 2.

Referring first to Figure 1, a computer network comprises a plurality of private access networks or intranets 230 and 240 interconnected by a public access network such as the Internet 10. A remote server 220 is connected to the Internet 10. Intranets 230 and 240 are connected to the Internet 10 via routers 20 and 30 respectively. Intranet 230 comprises a site network 40 which is connected to the Internet 10 via router 20. A proxy server 80 and an application server 210 are connected to local area or "site" network 40. Also connected to site network 40 is a plurality of user terminals represented here by user terminal 140. Intranet 190 comprises a plurality of site networks 50-70. Network 50 is connected to the Internet 10 via router 30. A proxy server 90 and an application server 190 are also connected to site network 50. Also connected to site network 50 is a plurality of user terminals represented here by user terminal 150. Site networks 60 and 70 are connected to site network 50 via routers 120 and 130 respectively. A proxy server 100 and an application server 180 are connected to site network 70. A plurality of user terminals, represented here by user

terminal 170, are also connected to site network 70. A proxy server 110 and an application server 200 are connected to site network 60. A plurality of user terminals, represented here by user terminal 160, are also connected to site network 60.

Each application server 180-200 provides application services such as printer services to user terminals connected to the corresponding site network 40-70. Each proxy server 80-110 provides network services to user terminals connected to the corresponding site network 40-70. In some embodiments of the present invention, proxy server and application server functions associated with a site network may be provided by a single computer connected to the site network. In other embodiments of the present invention however, proxy server and application server functions associated with a site network may be provided by a separate computers connected to the site network.

Data is communicated in the computer network between end-points such as user terminals 140-160 and application servers 180-210, in datagrams defined by the Transmission Control Protocol/Internet Protocol (TCP/IP). Each end-point, such as user terminal 140, is identified by a unique Internet Protocol (IP) address. As mentioned earlier, each datagram comprises a header portion and a data portion. The header portion contains the IP address of the source of the datagram and the IP address of the destination of the datagram. The data portion contains the data to be delivered.

Referring now to Figure 2, each router 20,30,120,130 in the computer network comprises a memory containing a routing table 260. In operation, the routing table 260 controls admission of datagrams from source IP addresses on a first sub-network, such as site network 40, to destination IP addresses on a second sub-network, such as the Internet 10, and vice versa. As simplified example of the routing table 260 is shown in the Table below.

TABLE

SOURCE ADDRESS	DESTINATION ADDRESS	PROTOCOL	ACTION
outside intranet	appln server	any	deny
outside intranet	user terminal	http or ftp	deny
outside intranet	user terminal	telnet	pass
outside intranet	proxy	any	pass
appln server	outside intranet	any	send to proxy
proxy	outside intranet	http or ftp	pass
user terminal	outside intranet	telnet	pass
user terminal	outside intranet	http or ftp	send to proxy

By way of example, the routing table 260 of router 20 will now be described with reference to the Table above. The routing table 260 is arranged such that any datagrams arriving from an IP address outside intranet 230 and destined for application server 210, are denied access to intranet 230 by router 20 regardless of protocol. However, according to the routing table any datagrams, regardless of protocol, which arrive from an IP address outside intranet 230, and which are destined for proxy server 80, are admitted to intranet 230 by router 20. Similarly, according to the routing table 260, http protocol datagrams from proxy server 80 are passed onto the Internet 10 by the router 20. By admitting some datagrams, but denying others, it will be appreciated that, by virtue of the configuration of routing table 260 hereinbefore described, router 20 provides a firewall function. Any datagrams from an external IP address destined for the user terminal 140 are denied access if the associated protocol should be handled by the proxy server 80. Any datagrams from an external IP address destined for the user terminal 140 are passed if the associated protocol is not handled by the proxy server, but acceptance is nevertheless desired. In accordance with the present invention, the routing table 260 re-routes any datagram arriving from the application server and destined for an IP address outside the intranet 230 to the proxy server 80. Similarly, the routing table 260 reroutes any datagrams sent from user terminal 140 to an IP address outside the intranet to the proxy server 80. Any datagrams re-routes by router 20 to the proxy server 80 are subsequently forwarded by the proxy server 140 to the IP address originally specified.

As mentioned earlier, conventionally, when a firewall is employed in to control access to a computer network such as intranet 40, users

generally have to modify the configuration, software and procedures on their terminals to access external networks such as Internet 10. However, as mentioned earlier, users may configure their terminals incorrectly. Also, network topologies can change leaving terminal configuration outdated. Furthermore, terminal configurations have to be changed as users move from one site to another. Such reconfigurations are time consuming and inconvenient, particularly although not exclusively in networking environments comprising a plurality of mobile user terminals such as lap top computers and personal digital assistants. In preferred embodiments of the present invention, this problem is solved at the firewall by rerouting all datagrams destined for external networks via a proxy server such as proxy server 40. The proxy server 40 then provides communications services between the source user terminal 140 and the destination on the external network 10 in a secure and controlled manner.

For example, with reference to Figure 3, suppose a browser 145 such as Netscape Navigator or IBM WebExplorer in user terminal 140 is configured to send a datagram 270 to a web page 225 on remote server 220 independently of proxy server 80. The routing table 260 in router 20 blocks delivery of the datagram 270. Referring now to Figure 4, in accordance with the present invention, router table 260 directs router 20 to divert the datagram 270 to proxy server 80. Referring now to Figure 5, proxy server 80 examines the datagram 270, performs any authentication required, and, if appropriate, forwards it, via router 20 to the remote server 220. In particular, the IP source address in the datagram is set to that of remote server 220 rather than proxy server 80.

If proxy server 80 is integral to router 20, then proxy server 80 simply opens another connection through the firewall to remote server 225, forwards the datagram 270, and receives any results, such as the contents of www page 225. Such results are then forwarded by proxy server 80 to the browser 145 in user terminal 140 with fields marked as if they were sent directly by remote server 220.

If proxy server 80 runs on a different machine to router 20, then datagrams rerouted by router 20 to proxy server 80 are re-addressed by router 20. To preserve the original destination, in preferred embodiments of the present invention, rerouted datagrams are encapsulated in another datagram, so that the original address is maintained within the rerouted datagram for access by proxy server 80. In preferred embodiments of the present invention, such encapsulation is performed by computer program

code running on router 20. In particularly preferred embodiments of the present invention, TCP/IP facilities such as "proxy ARP" enable proxy server 80 to directly receive subsequent datagrams without processing at router 20. It will be appreciated that, apart from slight differences in programming interfaces for decoding intended destination addresses, proxy server software can remain unchanged from exiting proxy servers such as http, Telnet and ftp proxy servers.

Encapsulation is one way of preserving the relevant information. However, it should be appreciated that, in some embodiments of the present invention, other preservation techniques may be employed. For example, a translation program running on the router or the proxy server nay simulate a proxy request. This means that the http proxy server code can be standard, with the IP address modification contained in the translation and/or encapsulation software.

In preferred embodiments of the present invention, end users apparently have direct connections to remote servers. However, in reality, all such accesses are trapped, and security policy can thus be maintained despite changes in network topology. The rerouting function in preferred embodiments of the present invention avoids reconfiguration of user terminals in the event of network changes to maintain security functions.

Preferred embodiments of the present invention have been hereinbefore described with reference to a router disposed between an intranet and the Internet. However, referring back to Figure 1, it will be appreciated that the present invention is equally applicable to routers disposed between site networks within an intranet, such and routers 120 and 130. In such arrangements, the "reroute to proxy" function hereinbefore described may be employed in the interests of network management to track passage of data packets between site networks via network management software executing on proxy servers connected to such site networks. The reroute to proxy function may also economise on network bandwidth if the proxy server can store local cached copies of dat from remote servers. On request for a page from the remote server, the caching proxy server may determine if it has an up-to-date copy of the remote information and return that copy if so. This avoids requesting the data from the remote server, thereby reducing bandwidth usage in the Internet. Access to remote data is also expedited.

CLAIMS

1. Apparatus for routing a data packet received from a source on a first network having a proxy server and addressed to a destination on a second network, the apparatus comprising means for forwarding the data packet to the proxy server instead of the destination addressed in response to the data packet satisfying predetermined criteria.

2. Apparatus as claimed in claim 1, wherein the forwarding means comprising a routing table for storing the predetermined criteria.

3. Apparatus as claimed in claim 1 or claim 2, wherein the predetermined criteria comprises a source address on the first network.

4. Apparatus as claimed in any preceding claim, wherein the predetermined criteria comprises a destination address on the second network.

5. Apparatus as claimed in any preceding claim, wherein the predetermined criteria includes a protocol type of the data packet.

6. A router comprising apparatus as claimed in any preceding claim.

7. A method for routing a data packet, the method comprising: receiving the data packet from a source on a first network having a proxy server and addressed to a destination on a second network; and, forwarding the data packet to the proxy server instead of the destination addressed in response to the data packet satisfying predetermined criteria.

8. A method as claimed in claim 7, comprising storing the predetermined criteria in a routing table.

The Patent Office

-9-

Application No: GB 9723154.2 **Examiner:** Keith Williams
Claims searched: 1-8 **Date of search:** 4 March 1998

Patents Act 1977
Search Report under Section 17

Databases searched:

UK Patent Office collections, including GB, EP, WO & US patent specifications, in:

UK Cl (Ed.P): H4P (PPA, PPEB)

Int Cl (Ed.6): H04L 12/46, 12/56, 12/66, 29/06

Other: Online WPI

Documents considered to be relevant:

Category	Identity of document and relevant passage		Relevant to claims
A	GB 2309561 A	Trend Micro Inc. - see abstract (and WO97/12321 and US 5623600)	1,7
X	GB 2306862 A	Holborow - see page 3, lines 22-28 (and WO 97/16782)	1,7
A	EP 0570630 A1	Alcatel - see column 2, lines 25-43	1,3,4,7
X	EP 0511926 A1	IBM Corp. - see abstract	1,2,4,7
X	US 5623601	Milkway Networks Corp. - see abstract	1,4,7
A	US 5559883	Chipcom Corp. - see abstract	1-4,7

X	Document indicating lack of novelty or inventive step	A	Document indicating technological background and/or state of the art.
Y	Document indicating lack of inventive step if combined with one or more other documents of same category.	P	Document published on or after the declared priority date but before the filing date of this invention.
&	Member of the same patent family	E	Patent document published on or after, but with priority date earlier than, the filing date of this application.